DoD Joint Federated Assurance Center (JFAC) Update

Thomas D. Hurt

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

19th Annual NDIA Systems Engineering Conference

Springfield, VA | October 26, 2016

JFAC Mission

The JFAC is a federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities. The JFAC member organizations and their technical service providers interact with program offices and other interested parties to provide software and hardware assurance expertise and support, to include vulnerability assessment, detection, analysis, and remediation services, and information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices.

JFAC Goals, Functions and Objectives

Goals

- Operationalize and institutionalize assurance capabilities
- Organize to better leverage the DoD, interagency, and public/private sector capabilities
- Influence R&D investments and activities to improve assurance

Functions

- Support Program Offices and Systems across the Lifecycle
- Sustain inventory of SwA and HwA resources across DoD
- Coordinate R&D agenda for assurance (software, hardware, firmware, systems, services, mission)
- Procure, manage and enable access to enterprise licenses for vulnerability analysis and other tools
- Communicate assurance expectations to broader communities of interest and practice

Objectives: Reduce program risks, costs

- Grow DoD competency and practice in SwA and HwA tools, techniques, and practices
- Assurance issue resolution through community collaboration, support, and remediation best-practice
- Leverage commercial products, methods, and training
- Provide practice-based guidance to tailor SwA and HwA to program needs in contracts
- Raise the bar on reduction of vulnerabilities and defects through spread of best practice
- Heighten SwA awareness through outreach, mentoring, training, education, and providing SwA tools
- Assess assurance capability gaps and recommend specific actions and products to close

Now implementing toward FOC

JFAC Implementation Progress

- **JFAC Charter**
  - ✓ Complete
- **JFAC Congressional Report**
  - ✓ Complete
- **CONOPS**
  - ✓ Complete
- **Draft SOPs**
  - ✓ Draft list of SOPs to be developed from use cases
  - ✓ Initial SOPs for SC, AO,TWGs, and JFAC-CC
- **JFAC Service Providers List**
  - ✓ Initial Mil Dep surveys underway
  - ✓ Initial insights provided to JFAC SC
- **DoD SwA Tool Licensing**
  - ✓ Drafted terms of reference
  - ✓ Put $1.17M on contract with USACE and acquire
  - ✓ Initial set of Licenses procured and distributed via JFAC Portal
- **NIPR and SIPR Portal Sites**
  - ✓ NIPR Portal structured
  - ✓ Hosting established (AMRDEC)
  - ✓ Developing content
  - ✓ SIPR- Site hosting & tools in-process at AMRDEC
- **JFAC Funding Plan**
  - ✓ Initial funding established and allocated
  - ✓ Need continued leadership involvement/support
- **JFAC-CC SOW (Competition Plan)**
  - ✓ Core group of service leads established
  - ✓ Strategy for sections C, L and M
  - ✓ Transition to SEI
  - ✓ Plan for long term solution in progress
- **JFAC SwA and HwA TWGs**
  - ✓ SwA TWG operating per CONOPS and initial SOPs
  - ✓ HwA TWG operating per CONOPS and initial SOPs
- **Draft DoD-wide SwA and HwA capability maps**
  - ✓ HW WG develop initial capability maps
  - ✓ SW WG develop interim capability maps
  - ✓ HW capability map provided to ASD(R&E)
- **Initial Strategic Plan**
  - ✓ Proposed outline developed and approved by AO WG
  - ✓ Initial draft plan in development
- **JFAC/R&D Interactions -- Enterprise Solutions**
  - ✓ Process in planning for assessing and informing R&D of JFAC operational gaps and needs

As of 10 April 2016

JFAC Achieved IOC 10 April 2016

SwA Tool Enterprise Licensing Initiative

- **Problem:**
  - Application of software assurance tools and techniques across DoD is inconsistent -- and often after engineering and development are completed, and when few resources are available for remediation
  - Expertise of best practices is isolated in various programs
  - Cost of SwA tools and lack of general knowledge about how to properly use them hampers widespread adoption
  - Use of SwA tools is not optimized for remediation of vulnerabilities by engineers

- **Solution: Break down barriers to wider adoption of SwA tools and practices throughout DoD**
  - Developers conducting demos of SwA tools to JFAC community
  - Request industry support to providing more demos and tool information
  - Implement enterprise licenses of SwA tools to promote wider and better use
  - Provide training and expertise to engineers and developers for why, how, and when to best use SwA tools
  - Simplify acquisition of SwA tools by moving from thousands of individual program and organization potential acquisitions across DoD to 1 per vendor
  - Simplify use of SwA tools by providing one centralized automated ticket-based request and download mechanism available throughout DoD, including direct support contractors
- **Status: Current pilot in operation => Transition to enterprise solutions**

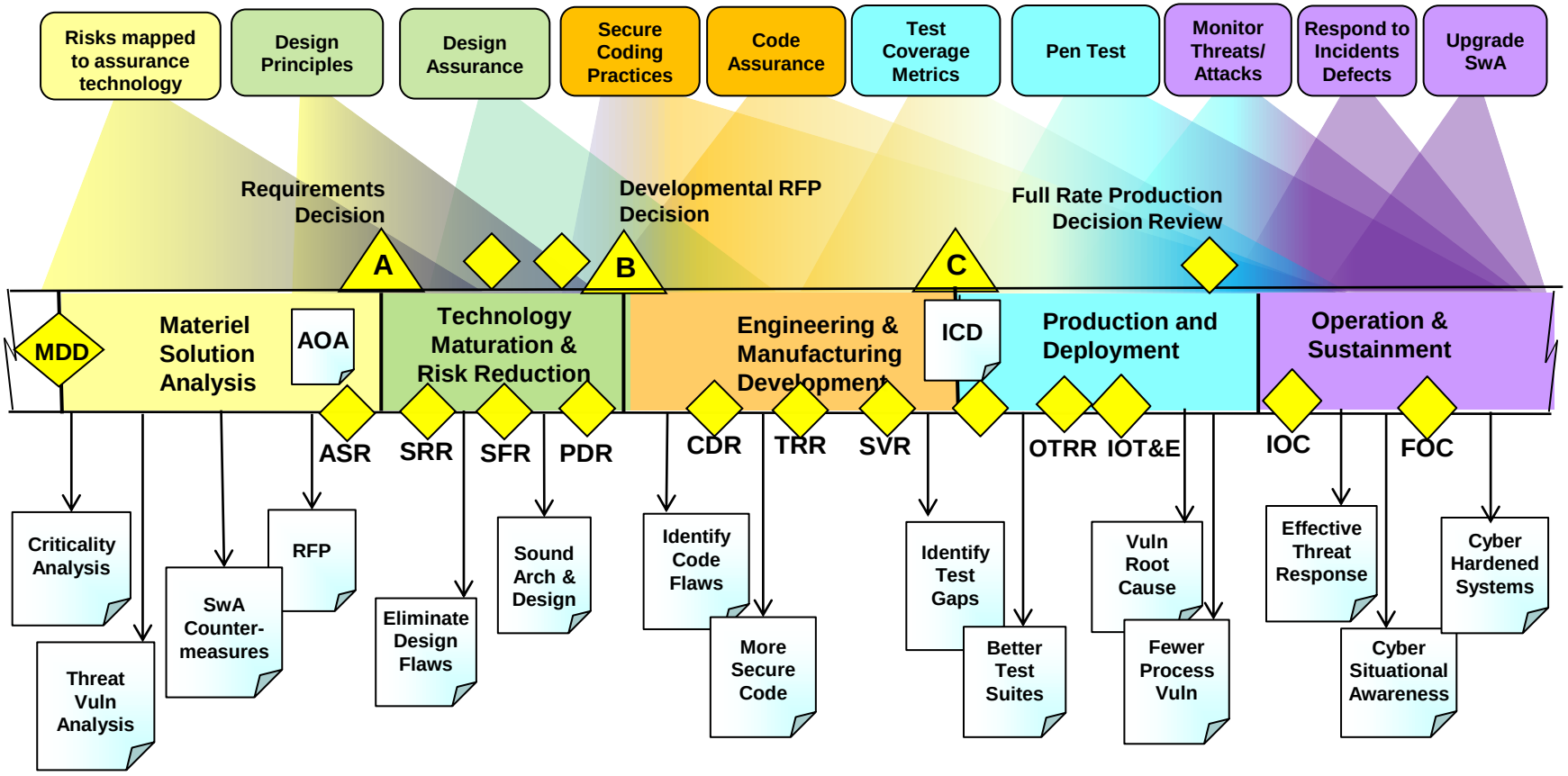
SwA Tool Acquisition and implementation Strategy

- **JFAC SwA Technical Working Group (TWG) is developing a SwA tool and license procurement strategy**
  - Focus on addressing current gaps and weaknesses in DoD SwA assessment and mitigation capabilities
  - Give special emphasis to supporting smaller acquisition and development programs in need of specialized SwA tools and services
- **TWG will also review and assess open source SwA tools that potentially could help offset some of the larger, tool purchase requirements**
  - Work with NSA's Center for Assured Software (CAS) to address potential concerns about the security and integrity of the open source products.

JFAC TASK	TIME
• Conduct SwA Tool Assessment and Use/Need Survey	01-2017
• Plan for "Industry Day" for developers and users to exchange ideas on working a centralized management, distribution, and tracking of engineering tools	05-2017
• Compile user and developer findings and inputs, comment, and develop acquisition documents	09-2017
• Acquire SwA tool enterprise licenses	FY18-on
• Distribute licenses via the JFAC ticketing system and portal automation	FY18-on
• Secure tool and license updates and renewals per community feedback	Each FY

Software Assurance for DoD Systems

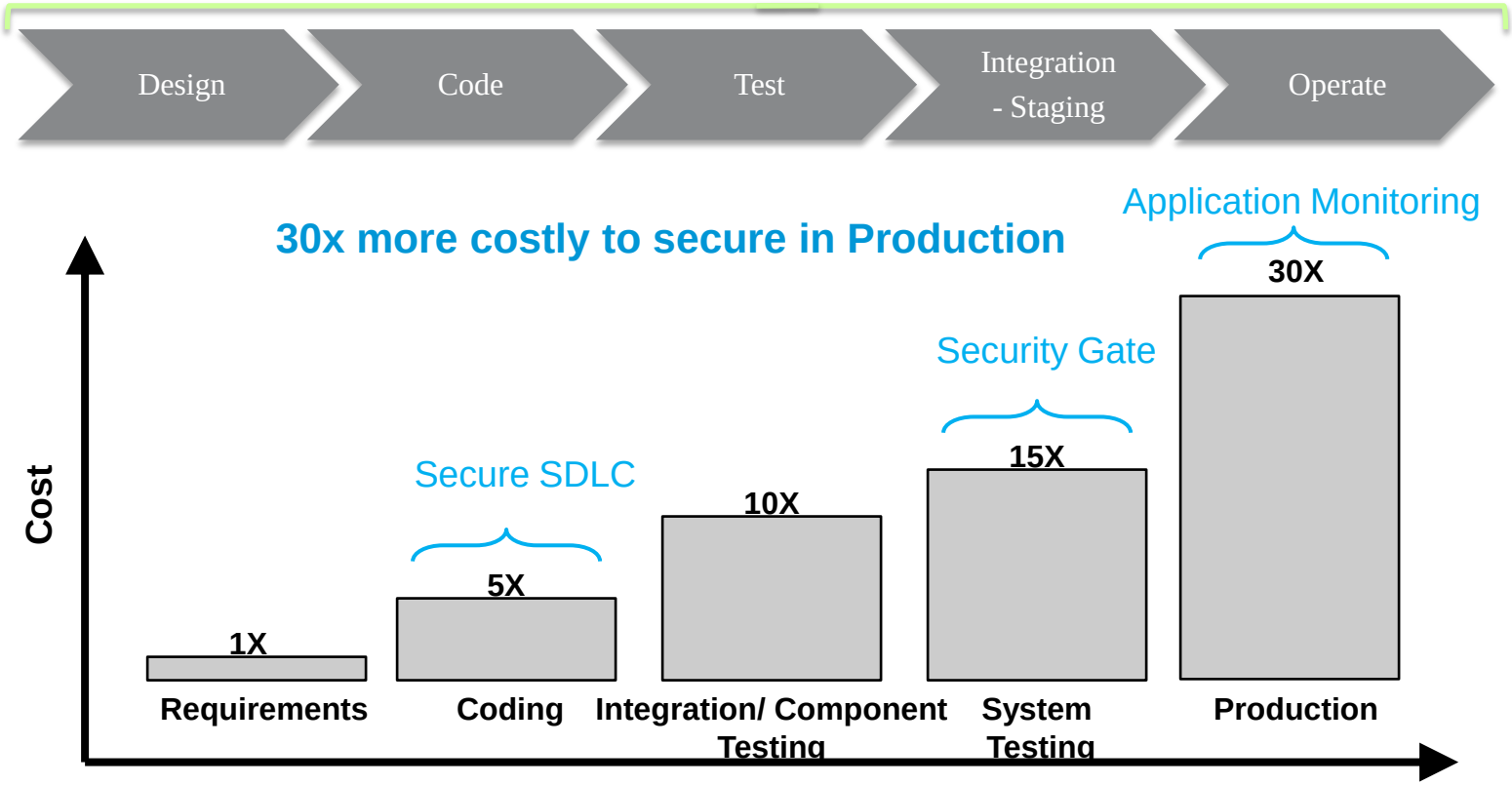
Software Assurance is SE focused on eliminating SW vulnerabilities



Implementation of Software Assurance must span the entire system lifecycle

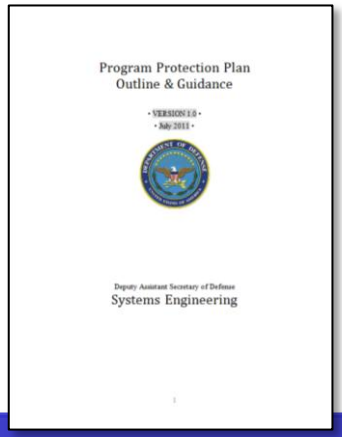
Value of Early Adoption of SwA

Cost-effective implementation of SwA means starting early



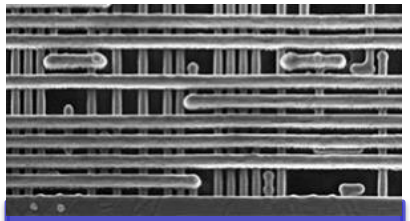
Source: NIST

Advancing Hardware Assurance



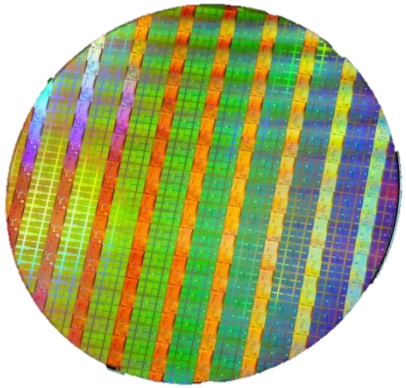
Policy

- DoD Instruction (DoDI) 5000.02
- Program Protection Plan (PPP)
- International Traffic in Arms Regulations (ITAR) update (in work)



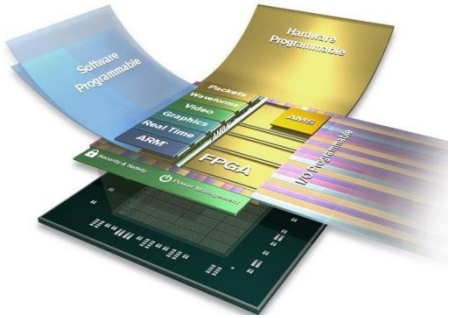
Joint Federated Assurance Center

- Software assurance Know-how & tools
- Hardware assurance Know how & tools
- Advanced V & V capabilities
- Firmware Assurance planning



Trusted & Assured Microelectronics

- Access to state-of-the-art foundries
- Trust and assurance methods and demonstration
- Industrial best practices for assurance
- Implement



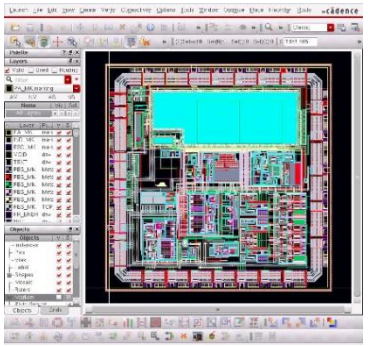
COTS and FGPA

- Supply chain risk management
- FPGA Assurance Study
- Radiation hardened microelectronics initiative

Microelectronics Trust Verification Technologies

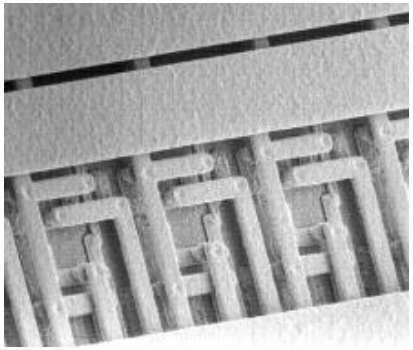
Design Verification

- Verification/assurance of designs, IP, netlists, bit-streams, firmware, etc.



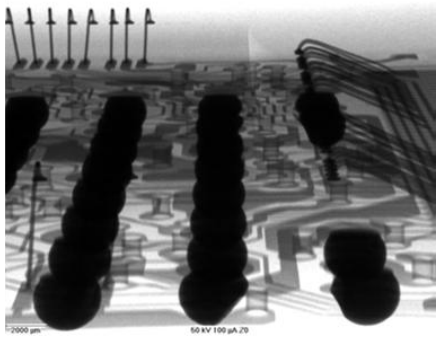
Physical Verification

- Destructive analysis of ICs and Printed Circuit Boards



Functional Verification

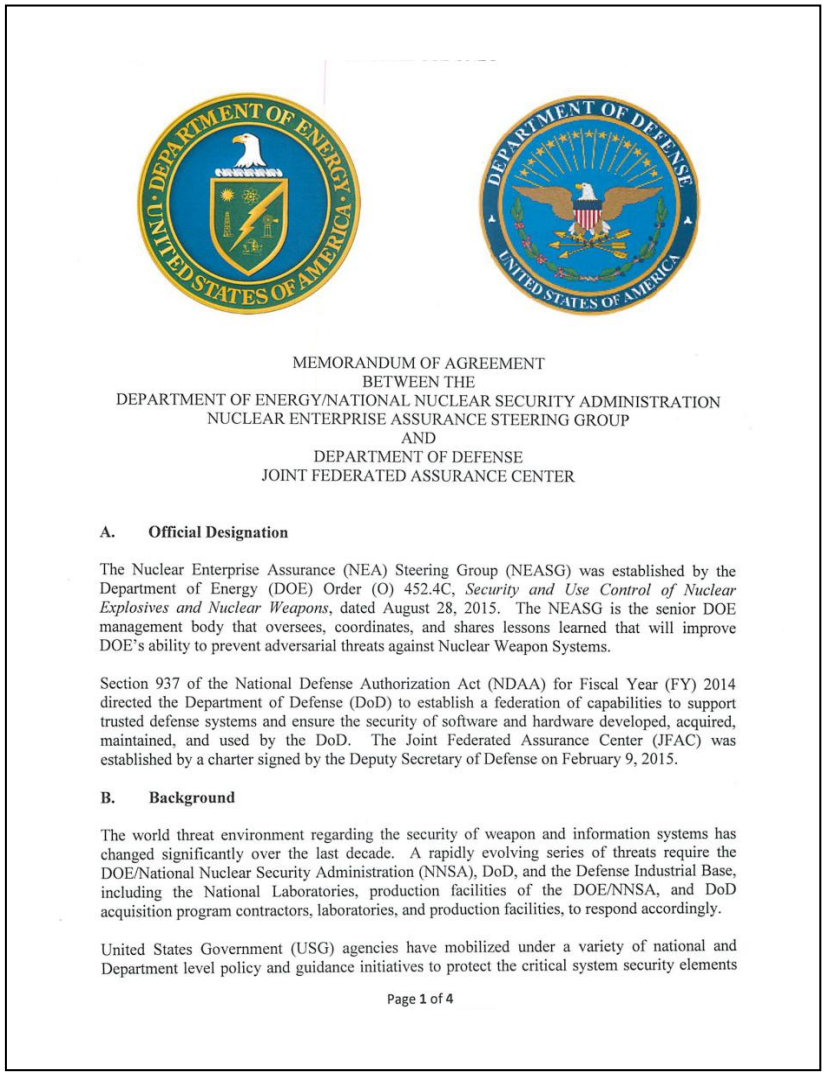
- Non-destructive screening and verification of select ICs



DoD, Intelligence Community, and DoE enhancing capability to meet future demand

JFAC MOA with DOE

- **MOA defines approach to coordination and sharing of HwA, SwA, SCRM, and WTA related policies, guidance, strategies, plans, implementation guidance, and other products**
- **Intended to help prevent malicious impacts to the supply chains, and better secure Nuclear Weapon Systems developed and deployed by DOE and DoD**
- **Also establishes JFAC website as the venue for collaboration among our respective subject matter experts to address shared issues, risks, and findings**



MEMORANDUM OF AGREEMENT
BETWEEN THE
DEPARTMENT OF ENERGY/NATIONAL NUCLEAR SECURITY ADMINISTRATION
NUCLEAR ENTERPRISE ASSURANCE STEERING GROUP
AND
DEPARTMENT OF DEFENSE
JOINT FEDERATED ASSURANCE CENTER

A. Official Designation

The Nuclear Enterprise Assurance (NEA) Steering Group (NEASG) was established by the Department of Energy (DOE) Order (O) 452.4C, *Security and Use Control of Nuclear Explosives and Nuclear Weapons*, dated August 28, 2015. The NEASG is the senior DOE management body that oversees, coordinates, and shares lessons learned that will improve DOE's ability to prevent adversarial threats against Nuclear Weapon Systems.

Section 937 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2014 directed the Department of Defense (DoD) to establish a federation of capabilities to support trusted defense systems and ensure the security of software and hardware developed, acquired, maintained, and used by the DoD. The Joint Federated Assurance Center (JFAC) was established by a charter signed by the Deputy Secretary of Defense on February 9, 2015.

B. Background

The world threat environment regarding the security of weapon and information systems has changed significantly over the last decade. A rapidly evolving series of threats require the DOE/National Nuclear Security Administration (NNSA), DoD, and the Defense Industrial Base, including the National Laboratories, production facilities of the DOE/NNSA, and DoD acquisition program contractors, laboratories, and production facilities, to respond accordingly.

United States Government (USG) agencies have mobilized under a variety of national and Department level policy and guidance initiatives to protect the critical system security elements

Page 1 of 4

JFAC Road to FOC

- **Program Planning**
  - JFAC Roadmap / Integrated Master Schedule
  - SW, HW and FW capability assessments and gap analyses
  - SwA tool assessment and procurement activities
  - FPGA assessments and strategy
  - Firmware study results and strategy
- **Program Engagement**
  - JFAC-CC aligned to support programs / portfolios
  - Program assessment and support capabilities
  - Assurance threat awareness and mitigation capabilities
  - Hard problem analysis and resolution capabilities
  - NIPR, SIPR and JWICS Portals
  - Interfaces with NSA, CERT, NIST
  - Surge / contingency capable
- **Service Providers**
  - Multiple go-to providers for assurance capabilities and services
  - Common criteria for assessing program needs
  - Established channels of communication and/or contracting with service providers
  - Agreed processes for nominating and assessing additional capability and service providers
- **Assurance Tools and Technologies**
  - Pilot Projects for SwA, HwA, and FwA
  - Enterprise Licenses Agreements (ELA)
  - ELA-like license processes for smaller business engagements
  - Contract Language available on JFAC Portal
  - Procurement, distribution, configuration control, and training activities
- **Community Outreach and Interaction**
  - **R&D Activities**
    - Mature, aligned and regularly interacting with other DoD, Mil Dep, and Defense Agency R&D activities
    - Focused on addressing identified assurance needs and gaps
  - **Integration with other Govt. Activities**
    - Collaborative problem solving (no free riders)
      - Formal MOAs
    - Interfaces w/Trusted Foundries / Cyber / Others
    - DoD / DOE Joint Firmware Study
  - **Interaction with Private Industry and Others**
    - NDIA SE Committee – Gaps, Methodologies, Best Practices
    - Academic, trade association, and other related communities of interest and practice

Summary

- **JFAC is a federation of DoD assurance capabilities and capacities**
  - To support programs in implementing assurance to mitigate cyber and supply chain attacks and vulnerabilities
  - To facilitate collaboration across the Department and throughout the lifecycle of acquisition programs
  - To maximize use of available resources
  - To assess and recommend capability and capacity gaps to resource
  - To coordinate assurance with organizations outside of DoD and industry
- **Innovation of SW and HW inspection, detection, analysis, risk assessment, and remediation tools and techniques**
  - R&D is key component of JFAC operations
  - Focus on improving tools, techniques, and procedures for SwA and HwA to support programs by including industry and academia
- **How You Can Help**
  - Continue to improve your own SW, HW and FW assurance capabilities and methodologies
  - Continue to partner with us to enable better awareness and collaboration in assurance tools, techniques and training

Support programs with SW, HW, and FW assurance

For Additional Information

Thomas D. Hurt

Deputy Director, Software Assurance and Software Engineering, DASD(SE)

571-372-6129 |

thomas.d.hurt.civ@mail.mil

JFAC Portal -- https://jfac.army.mil

Systems Engineering: Critical to Defense Acquisition





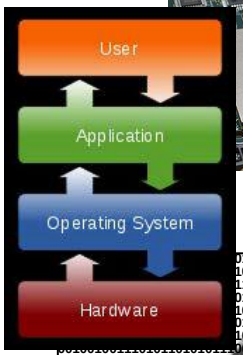





Defense Innovation Marketplace
http://www.defenseinnovationmarketplace.mil

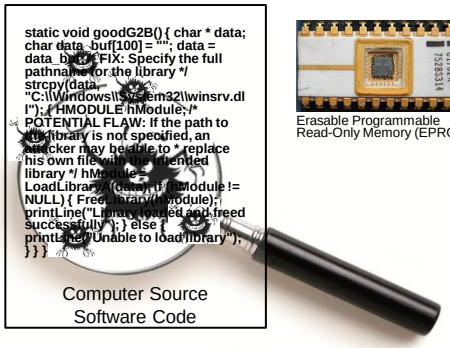
DASD, Systems Engineering
http://www.acq.osd.mil/se

Joint Federated Assurance Center (JFAC)



Field Programmable Gate Array

Binary Computer Software Code



Computer Source Software Code

Erasable Programmable Read-Only Memory (EPROM)

Build Assurance in

Intent:

- Congress directed DoD to "…provide for the establishment of a joint federation of capabilities to support the trusted defense system needs…to ensure security in the software and hardware developed, acquired, maintained, and used by the Department." (FY14 NDAA, Sect. 937)

Desired Outcomes/Deliverables:

- Federated cross-DoD awareness and coordination of software and hardware assurance (SwA/HwA) capabilities, information, resources, and expertise
- Development and sharing of SwA/HwA vulnerability assessment and remediation best practices, tested tools, and proven processes
- Identification of R&D needs to advance SwA/HwA capabilities for programs in acquisition, operational systems, and legacy systems and infrastructure
- Peer with other Government departments and agencies

Key Participants:

- Sponsor: ASD(R&E)/DASD(SE)
- Stakeholders: CIO, AF, Army, Navy, USMC, NSA, NRO, MDA, DISA, DMEA
- Interagency Relationships: DHS, DOE, DOC, CIA, NASA, GSA

Approach:

- Establish federation of SwA and HwA capabilities to promote software and hardware assurance in defense acquisition programs, systems, and supporting activities.
- Provide software and hardware assurance expertise and support, to include vulnerability detection, assessment, remediation, and test services; information about emerging threats and capabilities; software and hardware assessment tools and services, and best practices.
- Conduct Department-wide capability gap analysis to assess current SwA and HwA capabilities, identify opportunities, and bridge gaps.
- Coordinate with DoD R&D and other partners to identify potential areas of innovation for SwA and HwA technology.
- Procure, manage, and distribute DoD-wide, enterprise licenses for SwA and HwA analysis tools for use in each part of the life cycle.

Milestones:

Formed Steering Committee and Working Groups	07-2014
Initiated First Series of Technical Tasks	09-2014
Charter signed by Deputy Secretary of Defense	02-2015
Congressional Report signed & submitted	03-2015
JFAC CONOPS signed and distributed	10-2015
Initiate Capability Assessment, Gap Analysis, Strategic Planning processes	12-2015
JFAC Portal operational (https://jfac.army.mil)	12-2015
JFAC Coordination Center Transitions to SEI	01-2016
SwA License Pilot Project Launched	03-2016
Declaration of Joint Federated Assurance Center IOC	04-2016
MOA with DOE	08-2016